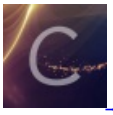
【jarvisoj刷题之旅】逆向题目[61dctf]stheasy的writeup

原创

iqiqiya 于 2018-09-09 16:57:34 发布 827 收藏 1
分类专栏： 我的逆向之路 我的CTF之路 我的CTF进阶之路 文章标签： 逆向题目[61dctf]stheasy的writeup stheasy 逆向题目[61dctf]stheasy的writeup reverse

本文链接：https://blog.csdn.net/xiangshangbashaonian/article/details/82559948

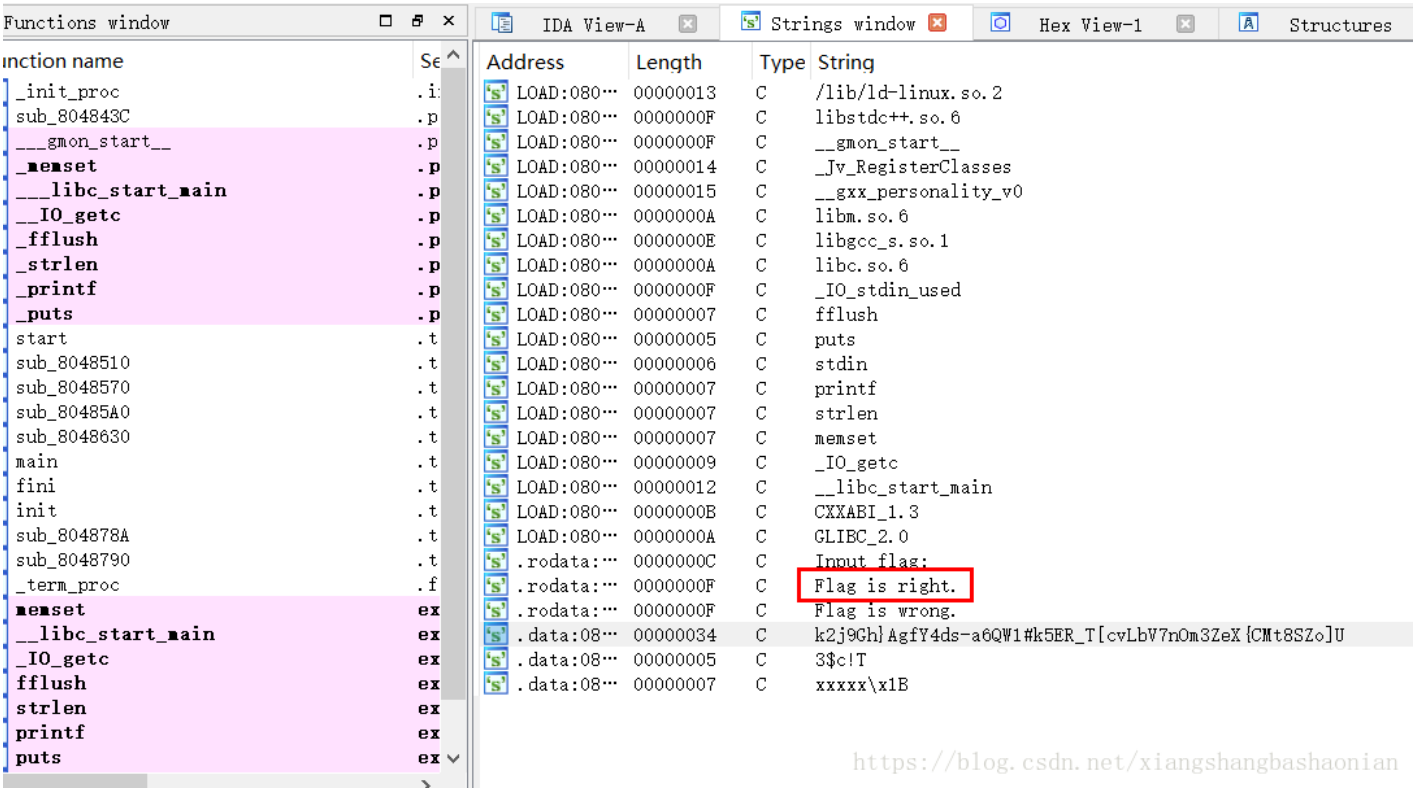

我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏

我的CTF进阶之路
108 篇文章 18 订阅
订阅专栏

直接载入IDA

看有没有什么可疑字符串



双击进入

```
.rodata:080487E3                db    0
.rodata:080487E4 ; char format[]
.rodata:080487E4 format          db 'Input flag:',0      ; DATA XREF: main+11↑o
.rodata:080487F0 ; char aFlagIsRight[]
.rodata:080487F0 aFlagIsRight    db 'Flag is right.',0   ; DATA XREF: main:loc_80486F8↑o
.rodata:080487FF ; char s[]
.rodata:080487FF s               db 'Flag is wrong.',0   ; DATA XREF: main+39↑o
.rodata:080487FF _rodata         ends
.rodata:080487FF
LOAD:0804880E ; ============================================================================
LOAD:0804880E
LOAD:0804880E ; Segment type: Pure code
```


双击进入引用

F5反汇编成c代码

经过分析可以看出sub_8048630()这个方法是关键

双击进入

IDA View-A | Pseudocode-B | Pseud

```
1  int __cdecl main()
2  {
3    char s; // [esp+10h] [ebp-110h]
4
5    printf("Input flag:");
6    sub_80485A0(&s, 0x100u);
7    if ( sub_8048630(&s) )
8      puts("Flag is right.");
9    else
10     puts("Flag is wrong.");
11   return 0;
12 }
```


经过分析　再将一些难看的变量名什么的修改下

就变成下图这个样子

IDA View-A | Pseudocode-A | Strings window | Hex View-1

```
1  int __cdecl sub_8048630(char *s)
2  {
3    size_t v1; // eax
4    int i; // edx
5
6    if ( s )
7    {
8      v1 = strlen(s);
9      if ( v1 )
10     {
11       if ( v1 == 29 )
12       {
13         i = 0;
14         while ( s[i] == b[(a[i] / 3u - 2)] )
15         {
16           if ( ++i == 29 )
17             return 1;
18         }
19       }
20     }
21   }
22   return 0;
23 }
```

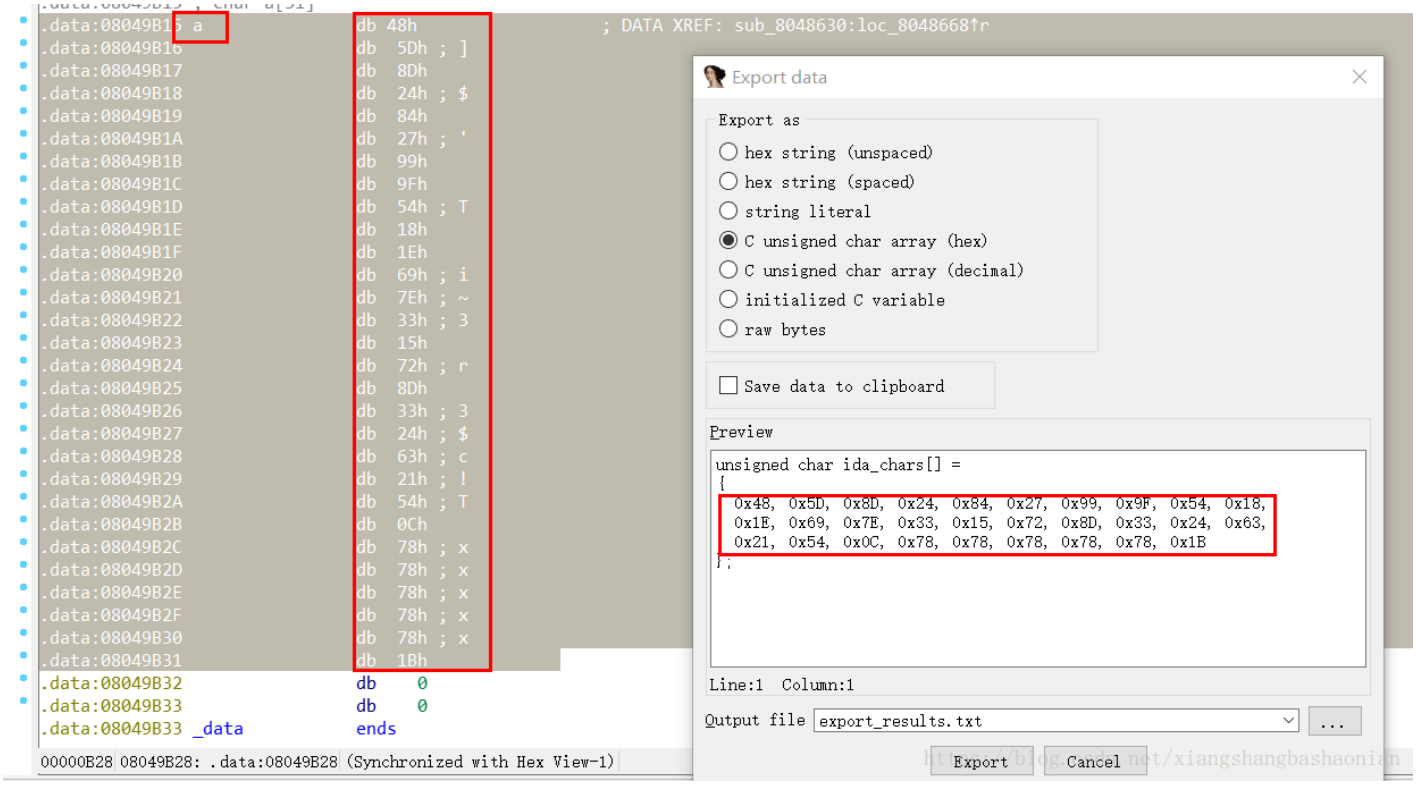
分析可知s就相当于我们想要得到的flag　反过来我们可以通过已经有的a和b这两个数组来得到flag

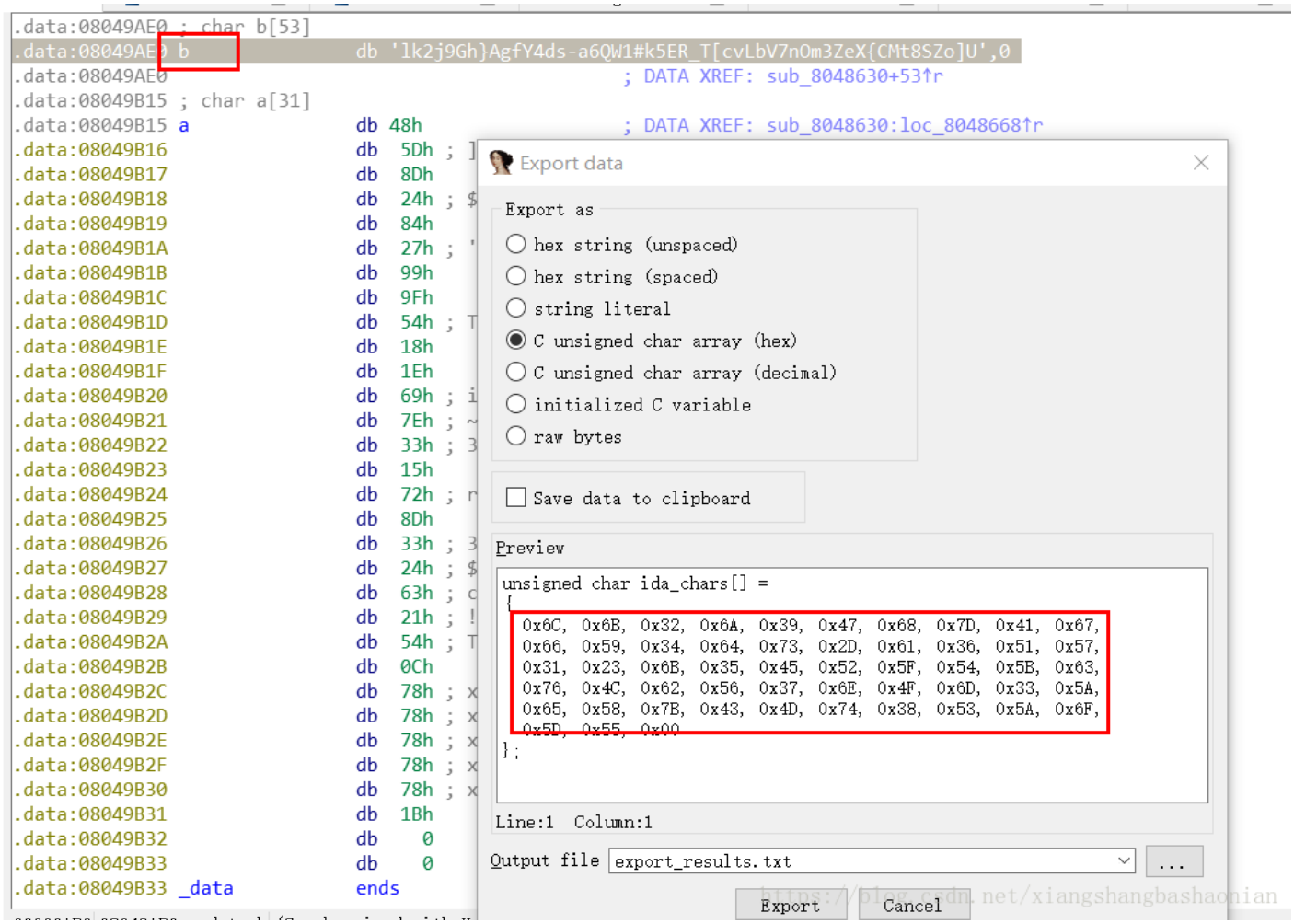
第一步：求a[i] / 3 -2　循环得到数组c(记得要将float转为int型)

第二步：求s[c[i]]　循环即可得到flag

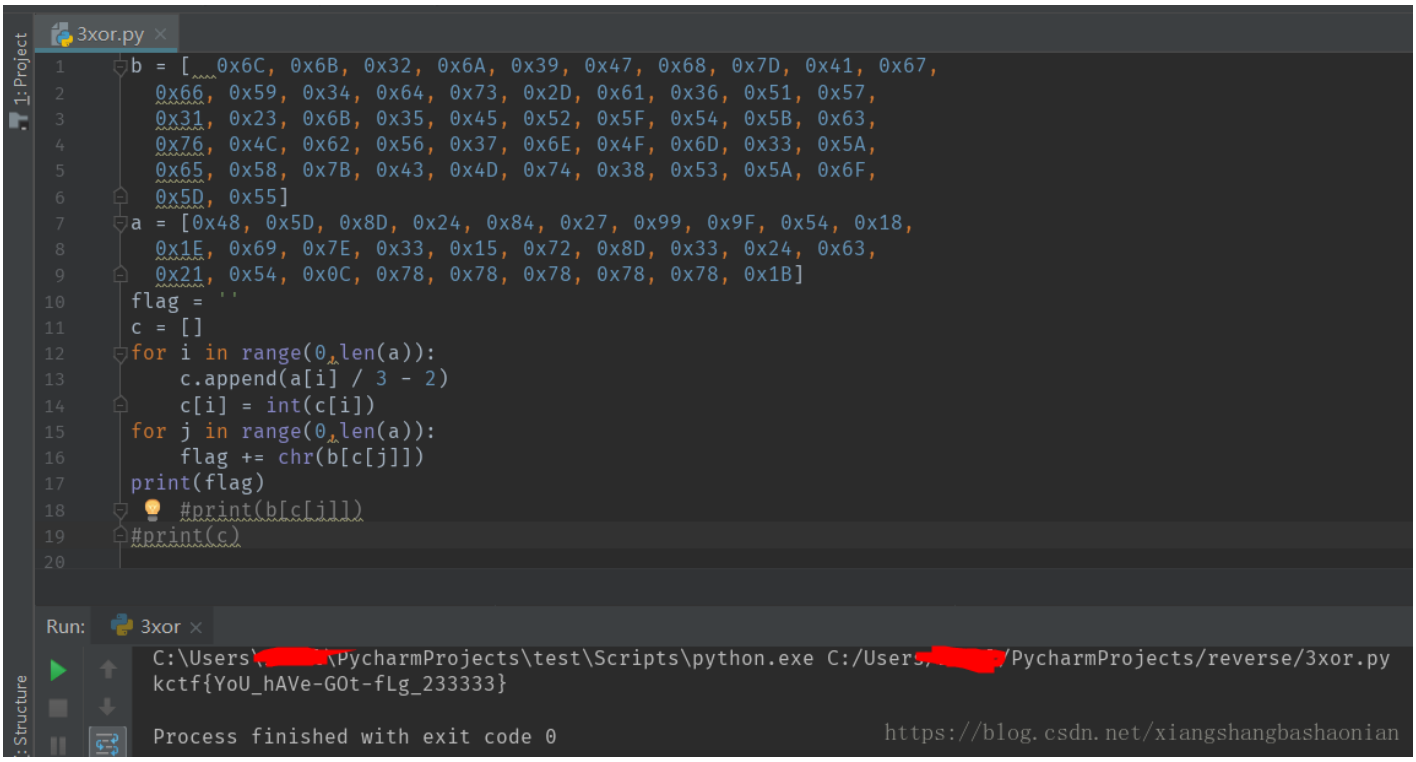
至于a,b的具体值可以双击进去找到

Shift+E就可以提取出来





Py大法好：



最后提交成功

[61dctf]stheasy

177 SOLVERS

100 REVERSE

ctf2.b93676be23733b2fcda3988c1133c1c1

kctf{YoU_hAVe-GOt-fLg_233333}

SUBMIT

Correct Answer!!Congratulations!